ABSTRACT OF THE DISCLOSURE

The present invention provides a novel configuration which allows devices capable of processing different signature algorithms to mutually verify public key certificates. In this configuration, public key certificates storing plural signatures based on different signature algorithms such as RSA and ECC are issued and each device selects a signature which can be processed (namely, verified) by itself and verifies the selected signature. Consequently, the novel configuration allows the devices each being capable of verifying only a different signature algorithm to verify the public key certificates of the other devices, so that each device can perform public key certificate verification in the cross-certification and encrypted data communication not only with the other devices having public key certificates attached with signatures based on the same signature algorithm as that of each device, but also with the other devices or providers having public key certificates attached with signatures based on different signature algorithms from that of each device, thereby significantly enhancing the reliability in communication.